Erste Beispiele: Wurzelgitter und Spiegelungsgruppen

Vortrag zum Seminar Gitter und Codes, 11.04.2011

Sascha Düerkop

Inhaltsverzeichnis

§1 Einführung

In diesem Kapitel werde ich zunächst einige wichtige Begriffe für die beiden Hauptkapitel einführen.

(1.1) Definition (Gitter)
Sei $E = (V, (,))$ ein euklidischer Vektorraum.

(i) Eine Teilmenge $L \subset V$ heißt *Gitter*, falls es ein linear unabhängiges Tupel $B = (b_1, \ldots, b_m) \in V^m$ gibt, mit

$$L = \langle b_1, \ldots, b_m \rangle_{\mathbb{Z}} = \{\sum_{i=1}^{m} a_i b_i | a_i \in \mathbb{Z}\}.$$

B heißt dann eine *Gitterbasis* von L und $m = \dim(L)$ die *Dimension* von L. L heißt *volles Gitter* in E, falls $\dim(L) = \dim(V)$, also wenn B eine Basis von V ist.

(ii) Ist $B \in V^m$ eine Gitterbasis von L und $\mathcal{G}(B) := ((b_i, b_j)) \in \mathbb{R}^{m \times m}$ die Grammatrix von B, so heißt

$$\det(L) := \det(\mathcal{G}(B))$$

die *Determinante* des Gitters L. $\mathcal{G}(B)$ nennt man auch eine *Grammatrix von* L.

(1.2) Bemerkung
Die Determinante eines Gitters ist wohldefiniert, obwohl die Gitterbasis nicht eindeutig ist. Seien B_1 und B_2 zwei Gitterbasen desselben Gitters L in ihrer Matrixdarstellung (d.h. die Zeilen der Matrix B_1 sind die Basisvektoren). Sei nun weiter M eine Basiswechselmatrix von B_1 nach B_2, d.h. es gilt $B_2 = MB_1$. Dann hat M Einträge in $\mathbb{Z}$ und die Determinante von M ist ± 1. Für die Determinante des Gitters bzgl. der gewählten Basis gilt nun also:

$$\det(L_{B_2}) = \det(\mathcal{G}(B_2)) = \det(B_2 B_2^T) = \det(M)^2 \det(B_1 B_1^T) = \det(L_{B_1})$$

(1.3) Beispiel
Das Standardbeispiel eines Gitters über $\mathbb{R}^n$ ist $\mathbb{Z}^n$. Dabei bilden die Einheitsvektoren $e_1, \ldots, e_n$ eine Gitterbasis von $\mathbb{Z}^n$.

(1.4) Definition und Lemma
Sei L ein volles Gitter in $E = (V, (,))$ mit Gitterbasis B. Dann ist

$$L^\# := \{v \in V | (v, l) \in \mathbb{Z} \text{ für alle } l \in L\}$$

auch ein volles Gitter in E. Man nennt $L^\#$ das zu L *duale Gitter*. Die Dualbasis $B^* = (b_1^*, \ldots b_n^*)$ von B ist eine Gitterbasis von $L^\#$.

Es gilt $\mathcal{G}(B)\mathcal{G}(B^*) = I_n$ und $\det(L^\#)\det(L) = 1$.
Ist $L \subset L^\#$, so nennt man das Gitter L *ganz*.
Die Faktorgruppe $L^\#/L$ ist dann eine endliche abelsche Gruppe der Ordnung $\det(L)$.
Es gilt $B^*\mathcal{G}(B) \in L^n$ und $\mathcal{G}(B)$ ist eine Relationenmatrix von $L^\#/L$. Sind $(d_1, \ldots, d_n)$ die Invariantenteiler von $\mathcal{G}(B)$, so ist $L^\#/L \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_n\mathbb{Z}$.

Beweis
Sei $v \in V$. Dann ist

$$(l, v) \in \mathbb{Z} \text{ für alle } l \in L \Leftrightarrow a_i := (b_i, v) \in \mathbb{Z} \text{ für alle } 1 \leq i \leq n \Leftrightarrow v = \sum a_i b_i^* \in \langle b_1^*, \ldots b_n^* \rangle_{\mathbb{Z}}$$

Also ist das duale Gitter $L^\#$ genau das von der dualen Basis erzeugte Gitter. Weiter ist ${}_{B^*}id_B = \mathcal{G}(B)$ die Basiswechselmatrix, d.h. $B^*\mathcal{G}(B) = B$. Damit ist $\mathcal{G}(B)$ die Relationenmatrix von $L^\#/L$ und $\det(\mathcal{G}(B)) = |L^\#/L|$. Die Elementarteiler von $\mathcal{G}(B) \in \mathbb{Z}^{n\times n}$ geben die Struktur der endlichen abelschen Gruppe $L^\#/L$ an. □

§2 Wurzelgitter

In diesem Kapitel werde ich zunächst das Wurzelgitter und Fundamentalsysteme von Wurzeln einführen und anschließend mit dem Satz von Witt eine Möglichkeit aufzeigen, eine im gewissen Sinne einfache Basis eines Wurzelgitters zu finden.

(2.1) Definition

(i) Ein ganzes Gitter L heißt *Wurzelgitter*, falls $L = \langle \{l \in L | (l, l) = 2\} \rangle_{\mathbb{Z}}$.

(ii) $L_{=2} := R(L) := \{l \in L | (l, l) = 2\}$ heißt die Menge der *Wurzeln* in L.

(iii) Eine Teilmenge $S \subset R(L)$ heißt *Fundamentalsystem von Wurzeln*, falls

(a) S ist Gitterbasis von L.

(b) Jede Wurzel $\beta \in R(L)$ lässt sich schreiben als

$$\beta = \sum_{\alpha \in S} k_\alpha \alpha \text{ mit allen } k_\alpha \geq 0 \text{ oder allen } k_\alpha \leq 0.$$

(2.2) Satz (Witt)
Ist L ein Wurzelgitter, so hat L eine Gitterbasis $B = (b_1, \ldots, b_n)$ mit $(b_i, b_i) = 2$ und $(b_i, b_j) \in \{0, -1\}$ für $1 \leq i \neq j \leq n$.
Jedes Fundamentalsystem von Wurzeln liefert eine solche Gitterbasis.

Beweis
Seien α, β Wurzeln des Wurzelgitters L.
Nach der Cauchy-Schwartz-Ungleichung gilt dann:

$$(\alpha, \beta)^2 \leq (\alpha, \alpha)(\beta, \beta) = 4.$$

Das heißt es ist $(\alpha, \beta) \in \{0, \pm 1, \pm 2\}$ und $(\alpha, \beta) = \pm 2$ genau dann wenn $\alpha = \pm\beta$.

Sei nun S ein Fundamentalsystem von Wurzeln und seien weiter $\alpha, \beta \in S$ und $\alpha \neq \beta$. Ist $(\alpha, \beta) > 0$ so ist $(\alpha, \beta) = 1$ und $\gamma = \alpha - \beta \in R(L)$ eine Wurzel, deren Koeffizienten bzgl. S weder alle nichtnegativ noch alle nichtpositiv sind.
Es bleibt also nur noch zu zeigen, dass ein Fundamentalsystem von Wurzeln existiert. Dieses kann wie folgt konstruiert werden:
Sei $t \in E$ so dass $(t, \alpha) \neq 0$ für alle $\alpha \in R(L)$. Ein solches t existiert stets, da die Menge

$$\{t \in E |\ \exists \alpha \in R(L) \text{ mit} (t, \alpha) = 0\}$$

als endliche Vereinigung von Hyperebenen nicht der gesamte Raum sein kann.
Sei nun $R_t^+ := \{\alpha \in R(L) | (t, \alpha) > 0\}$. Dann ist $R(L) = R_t^+ \cup -R_t^+$.
Ein Element $\alpha \in R_t^+$ heißt zerlegbar, falls es $\beta, \gamma \in R_t^+$ gibt, mit $\alpha = \beta + \gamma$. Sei nun $S_t := \{\alpha \in R_t^+ | \alpha \text{ ist nicht zerlegbar } \}$.
Behauptung: S_t ist ein Fundamentalsystem von L. Dazu sind zu zeigen:

(i) Jedes Element von R_t^+ ist eine Linearkombination von Elementen von S_t mit nichtnegativen Koeffizienten.

(ii) Für alle $\alpha \neq \beta \in S_t$ gilt $(\alpha, \beta) \leq 0$

(iii) Die Elemente von S_t sind linear unabhängig.

Sind diese drei Aussagen bewiesen, so folgt die Behauptung, da damit nach (i) und (ii) S_t ein Fundamentalsystem von Wurzeln ist und nach (i) + (iii) dieses auch wie gefordert eine Gitterbasis ist.
Nun also zu den Beweisen der drei Aussagen:

zu (i) Angenommen es existieren Elemente in R_t^+, die keine Linearkombination von Elementen von S_t ist.
Sei o.B.d.A $\alpha \in R_t^+$ eines dieser Elemente, so dass (α, t) minimal ist.
Dann ist α zerlegbar. Also gibt es $\beta, \gamma \in R_t^+$ mit $\alpha = \beta + \gamma$.
Somit gilt $(t, \alpha) = (t, \beta) + (t, \gamma)$ und $(t, \beta), (t, \gamma) < (t, \alpha)$. Wegen der Minimalität von α sind also β und γ nichtnegative Linearkombinationen von Elementen aus R_t^+, und damit auch α, was ein Widerspruch zur Annahme ist.

zu (ii) Angenommen es existieren $\alpha \neq \beta \in S_t$ mit $(\alpha, \beta) > 0$.
Dann ist $(\alpha, \beta) = 1$ und somit $\gamma := \alpha - \beta \in R_t^+$ oder $-\gamma \in R_t^+$.
Im ersten Fall ist $\alpha = \beta + \gamma$ zerlegbar und somit nicht in S_t und im zweiten Fall ist $\beta = \alpha + (-\gamma)$ zerlegbar und somit nicht in S_t. Beides liefert einen Widerspruch zur Annahme.

zu (iii) Angenommen die Elemente von S_t sind linear abhängig. Dann gibt es a_α, so dass $\sum_{\alpha \in S_t} a_\alpha \alpha = 0$.
Dann lässt sich diese Relation umschreiben als

$$\lambda := \sum b_\beta \beta = \sum c_\gamma \gamma$$

wobei $b_\beta, c_\gamma > 0$ und alle β von allen γ verschieden sind. Es ist

$$0 \leq (\lambda, \lambda) = \sum_{\beta,\gamma} b_\beta c_\gamma (\beta, \gamma) \leq 0$$

also $(\lambda, \lambda) = 0$ und somit $\lambda = 0$. Dann ist aber auch

$$(t, \lambda) = \sum b_\beta (t, \beta) = \sum c_\gamma (t, \gamma) = 0$$

also $b_\beta = c_\gamma = 0$ für alle β, γ
Dies steht im Widerspruch zur Annahme und somit sind die Elemente von S_t linear unabhängig. □

(2.3) Bemerkung
Im obigen Beweis geht implizit ein, dass $R(L)$ eine endliche Menge ist. Allgemein gilt sogar, dass die Menge

$$L_{\leq c} := \{x \in L | (x, x) \leq c\}$$

für alle $c \in \mathbb{R}_0^+$ eine endliche Menge ist.

Beweis
Aus der Analysis ist bekannt, dass die Kugel $B_c(0) = \{x \in V | (x, x) \leq c\}$ kompakt ist.
Somit ist dann $L_{\leq c} = B_c(0) \cap L$ kompakt und diskret, also endlich. □

— *Klassifikation von Wurzelgittern* —

In diesem Abschnitt wird sich zeigen, dass sich die möglichen Systeme $\{b_1, \ldots, b_n\}$, welche die Eigenschaften des Satzes von Witt erfüllen, mit Hilfe von Graphen klassifizieren lassen.

(2.4) Definition

1. Sei V ein $\mathbb{R}$-Vektorraum. Dann ist

$$\mathcal{O}(V) := \{\phi \in \mathrm{End}_{\mathbb{R}}(V) | (x, y) = (\phi(x), \phi(y)) \forall x, y \in V\}$$

die *orthogonale Gruppe* von V.

2. Sei L ein Gitter in V. Dann ist die *Automorphismengruppe* von L definiert als:
$$\mathrm{Aut}(L) := \{\phi \in \mathcal{O}(V) | \phi(L) = L\}$$
3. Seien L und L' volle Gitter in E. Dann heißen L und L' *isometrisch* falls es ein $g \in \mathcal{O}(E)$ mit $Lg = L'$ gibt.

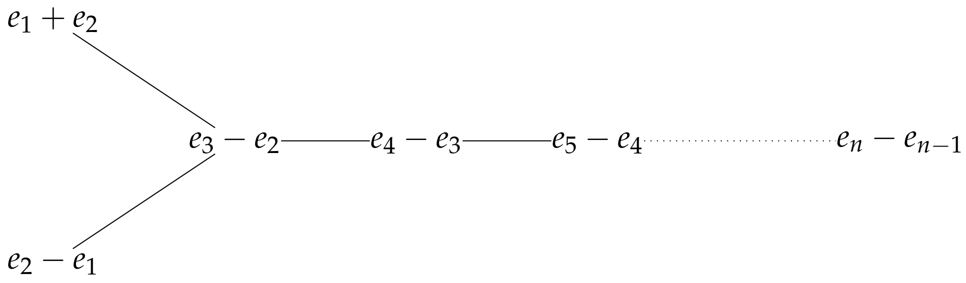
(2.5) Definition (Coxeter-Dynkin-Graph)
Zu jedem Fundamentalsystem von Wurzeln $\{b_1, \ldots, b_n\}$ sei der *Coxeter-Dynkin-Graph* folgendermaßen definiert:
Jedes Basiselement b_i bildet einen Knoten und die Kanten zwischen zwei Knoten seien durch die folgende Regel definiert für $i \neq j$:
$$(b_i, b_j) = -1 \Leftrightarrow b_i \text{———} b_j$$
$$(b_i, b_j) = 0 \Leftrightarrow b_i \qquad b_j$$

(2.6) Beispiele (Wurzelgitter)
(I) Betrachte den $\mathbb{R}^{n+1}$ mit der Standardbasis $\{e_1, \ldots, e_{n+1}\}$. Sei weiter
$$\epsilon := \sum_{i=1}^{n+1} e_i = (1, 1, \ldots, 1) \in \mathbb{R}^{n+1}.$$
Nun sei $\mathbb{A}_n$ wie folgt als Gitter in $\langle\epsilon\rangle^\perp$ definiert:
$$\mathbb{A}_n := \{x = (x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} | (x, \epsilon) = x_1 + \ldots + x_{n+1} = 0\}.$$
Dieses Gitter wird von den $n(n+1)$ Elementen $b_{i,j} := e_i - e_j$ $(1 \leq i, j \leq n+1, i \neq j)$ erzeugt.
Die Menge $\{e_2 - e_1, e_3 - e_2, \ldots, e_{n+1} - e_n\}$ ist eine Basis von $\mathbb{A}_n$ mit dem Coxeter-Dynkin-Graphen
$$b_{2,1} \text{———} b_{3,2} \text{———} b_{4,3} \cdots\cdots\cdots b_{n+1,n}.$$
Die Grammatrix dieser Basis ist gegeben durch:
$$\mathcal{G}(\mathbb{A}_n) := \begin{pmatrix} 2 & -1 & 0 & \ldots & \ldots & 0 \\ -1 & 2 & -1 & 0 & \ldots & 0 \\ 0 & -1 & 2 & -1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & -1 & 2 & -1 \\ 0 & \ldots & \ldots & 0 & -1 & 2 \end{pmatrix}$$
Induktiv ergbit sich $\det(\mathbb{A}_n) = n + 1$.
Da der Vektor $v := \frac{1}{n+1}(ne_1 - e_2 - e_3 - \ldots - e_{n+1})$ im dualen Gitter $\mathbb{A}_n^\#$ enthalten ist und $(n+1)v \in \mathbb{A}_n$ gilt, ist die Faktorgruppe $\mathbb{A}_n^\# / \mathbb{A}_n$ isomorph zu $\mathbb{Z}/(n+1)\mathbb{Z}$.

(II) Für $n \geq 3$ sei

$$\mathbb{D}_n := \{(x_1, \ldots, x_n) \in \mathbb{Z}^n | x_1 + \ldots + x_n \text{ ist gerade.}\}$$

Dann ist $\mathbb{D}_n$ ein Gitter in $\mathbb{R}^n$, welches von den $2n(n-1)$ Wurzeln $\pm e_i \pm e_j$ $(1 \leq i, j \leq n, i \neq j)$ erzeugt wird. Die Menge $\{e_2 - e_1, e_3 - e_2, \ldots, e_n - e_{n-1}, e_1 + e_2\}$ ist eine Basis von $\mathbb{D}_n$ und der Coxeter-Dynkin-Graph ergibt sich wie folgt:

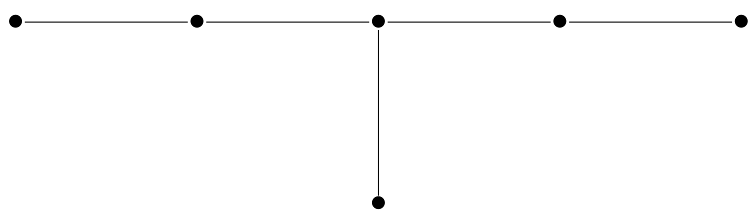


Demnach ist die Grammatrix der obigen Basis gegeben durch

$$\mathcal{G}(\mathbb{D}_n) = \begin{pmatrix} 2 & 0 & -1 & 0 & \ldots & \ldots & 0 \\ 0 & 2 & -1 & 0 & \ldots & \ldots & 0 \\ -1 & -1 & 2 & -1 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & -1 & 2 & -1 & 0 \\ 0 & 0 & \ldots & 0 & -1 & 2 & -1 \\ 0 & 0 & \ldots & \ldots & 0 & -1 & 2 \end{pmatrix}$$

Für die Determinante ergibt sich hier, ebenfalls induktiv: $\det(\mathbb{D}_n) = 4$.
Sei $v := \frac{1}{2}(e_1 + e_2 + \ldots e_n) \in \mathbb{D}_n^\#$. Dann ist $2v \in \mathbb{D}_n$ genau dann, wenn n gerade ist. Das bedeutet, dass $\mathbb{D}_n^\# / \mathbb{D}_n \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ gilt, falls n gerade ist und sonst $\mathbb{D}_n^\# / \mathbb{D}_n \cong \mathbb{Z}/4\mathbb{Z}$ gilt.

(III) Ein spezielles Gitter der Dimension 6 ist das Wurzelgitter mit dem Coxeter-Dynkin-Graphen

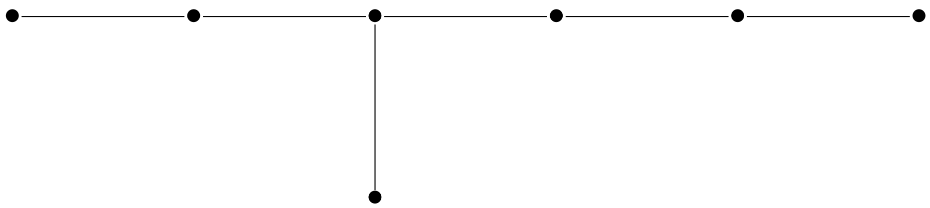


Die Grammatrix von $\mathbb{E}_6$ bezüglich der durch den Graphen beschrieben Basis lässt sich also bestimmen als

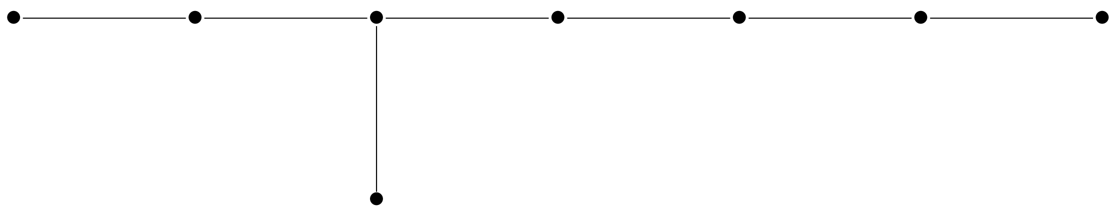
$$\mathcal{G}(\mathbb{E}_6) = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}$$

Die Determinante des Gitters lässt sich direkt berechnen als $\det(\mathbb{E}_6) = 3$.

Analog dazu lässt sich so ein spezielles Gitter auch in Dimension 7 konstruieren:



bzw. in Dimension 8:



Die Grammatrizen dieser Wurzelgitter sind ebenfalls analog zu $\mathbb{E}_6$:

$$\mathcal{G}(\mathbb{E}_7) = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 2 \end{pmatrix}$$

bzw.

$$\mathcal{G}(\mathbb{E}_8) = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

Als Determinanten ergeben sich hier $\det(\mathbb{E}_7) = 2$ und $\det(\mathbb{E}_8) = 1$.

(2.7) Definition (orthogonale Summe)

(i) Für zwei Gitter L_1, L_2 in den Vektorräumen V_1 bzw. V_2 bezeichnet $L_1 \perp L_2$ die (äußere) orthogonale Summe.
Dies ist ein Gitter in $V_1 \oplus V_2$ der Dimension $\dim(L_1) + \dim(L_2)$.
Sind $B = \{b_1, \dots b_{n_1}\}$ und $C = \{c_1, \dots c_{n_1}\}$ Gitterbasen von L_1 bzw. L_2, so ist $B' := \{(b_1, 0), \dots, (b_{n_1}, 0), (0, c_1), \dots, (0, c_{n_2})\}$ eine Gitterbasis von $L_1 \perp L_2$ mit Grammatrix

$$\mathcal{G}(B') = \begin{pmatrix} \mathcal{G}(B) & 0 \\ 0 & \mathcal{G}(C) \end{pmatrix}$$

(ii) Sind L_1, L_2 Gitter in V und $(l_1, l_2) = 0$ für alle $l_i \in L_i$, so heißt $L := L_1 \perp L_2 := \langle L_1, L_2 \rangle$ die (innere) orthogonale Summe.

(iii) Ein Gitter L heißt irreduzibel oder orthogonal unzerlegbar, falls L nicht orthogonale Summe echter Teilgitter ist.

Mithilfe dieser Definition lassen sich nun die Wurzelgitter klassifizieren:

(2.8) Satz
Jedes Wurzelgitter ist bis auf Isometrie eine orthogonale Summe der Wurzelgitter $\mathbb{A}_n$, $\mathbb{D}_n$ $(n \geq 4)$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$.

Beweis
vgl. Ebeling Theorem 1.2 (Seite 22) □

(2.9) Satz (Alternative)
Jedes irreduzible Wurzelgitter ist von der Form $\mathbb{A}_n$, $\mathbb{D}_n$ $(n \geq 4)$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$.

Zusammenfassend ist hier nochmal eine Tabelle gegeben, die die irreduziblen Wurzelgitter und ihre Eigenschaften kompakt darstellt:

Gitter L	$\lvert R(L)\rvert$	$\det(L)$	$L^\#/L$	Dimension n
$\mathbb{A}_n$	$n(n+1)$	$n+1$	$\mathbb{Z}/(n+1)\mathbb{Z}$	≥ 1
$\mathbb{D}_n$	$2n(n-1)$	4	$\mathbb{Z}/4\mathbb{Z}$	≥ 4, ungerade
$\mathbb{D}_n$	$2n(n-1)$	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	≥ 4, gerade
$\mathbb{E}_6$	72	3	$\mathbb{Z}/3\mathbb{Z}$	6
$\mathbb{E}_7$	126	2	$\mathbb{Z}/2\mathbb{Z}$	7
$\mathbb{E}_8$	240	1	1	8

§3 Spiegelungsgruppen

— *Weyl-Gruppe* —

Die in unserem interessante Spiegelungsgruppe ist die sogenannten Weyl-Gruppe, welche die Spiegelungsgruppe eines Wurzelgitter ist.

(3.1) Definition (Spiegelung und Weyl-Gruppe)
Sei L ein Wurzelgitter in V und sei $l \in L$ eine Wurzel.

(i) Die *Spiegelung* entlang l wird mit σ_l bezeichnet und ist für alle $v \in V$ wie folgt definiert:

$$v\sigma_l := v - 2\frac{(v,l)}{(l,l)}l = v - (v,l)l$$

Dies ist eine orthogonale Abbildung, die L festlässt, d.h. es gilt $\sigma_l \in \mathrm{Aut}(L)$.

(ii) Die Gruppe

$$W(L) := \langle \sigma_l | l \in R(L) \rangle \leq \mathrm{Aut}(L)$$

heißt *Weyl-Gruppe* von L. Da für alle Spiegelungen stets $g^{-1}\sigma_l g = \sigma_{gl}$ gilt, ist die Weyl-Gruppe sogar ein Normalteiler von $\mathrm{Aut}(L)$.

Einige interessante Eigenschaften der Weyl-Gruppe zeigen der folgende Satz und das darauf folgende Lemma:

(3.2) Satz
Sei L ein Wurzelgitter und $W(L)$ seine Weyl-Gruppe.
L ist genau dann irreduzibel wenn jeder $W(L)$-invariante Teilraum $U \leq V$ entweder der Nullvektorraum oder ganz V ist.

Beweis
$\Rightarrow$: Sei $\{0\} \neq U < V$ mit $Ug = U$ für alle $g \in W(L)$. Dann ist auch $U^\perp$ ein $W(L)$-invarianter Teilraum, da $W(L) \leq \mathcal{O}(V)$ und $V = U \oplus U^\perp$. Sei nun $\alpha \in R(L)$ und angenommen $\alpha \notin U$. Für $u \in U$ ist dann $u\sigma_\alpha = u - (u,\alpha)\alpha \in U$, da U invariant unter $W(L)$ ist. Also ist $(u,\alpha) = 0$ für alle $u \in U$ (da $\alpha \notin U$) und somit $\alpha \in U^\perp$. Das heißt jedes $\alpha \in R(L)$ liegt in U oder $U^\perp$, also ist L reduzibel.
Dies ist ein Widerspruch zur Annahme und somit folgt die Behauptung.

$\Leftarrow$: Angenommen L ist irreduzibel, also $L = L_1 \perp L_2$. Dann ist $U := \mathbb{R}L_1$ ein $W(L)$-invarianter Teilraum von V. Denn es ist dann $R(L) = R(L_1) \cup R(L_2)$. Somit ist für $u \in U$ und $\alpha \in R(L_2)$

$$u\sigma_\alpha = u \in U \text{ und für } \alpha \in R(L_1) \text{ ist } u\sigma_\alpha \in U.$$

Also ist U ein $W(L)$-invarianter Teilraum und da $\{0\} \neq U \neq V$ gilt, ist dies ein Widerspruch zur Annahme. □

(3.3) Lemma
Sei L ein irreduzibles Wurzelgitter. Dann operiert die Weyl-Gruppe $W(L)$ von L transitiv auf den Wurzeln von L, also auf $R(L)$.
Das bedeutet, dass es für je zwei Wurzeln $\alpha, \beta \in R(L)$ ein $g \in W(L)$ gibt, so dass $\alpha g = \beta$ gilt.

Beweis
Seien $\alpha, \beta \in R(L)$. Dann ist $U := \langle \alpha g | g \in W(L) \rangle_{\mathbb{R}}$ ein $W(L)$-invarianter Teilraum von $\mathbb{R}L = V$. Nach dem vorigen Lemma ist also $U = V$. Die Bilder von α unter der Gruppenoperation erzeugen also den ganzen Raum. Daher gibt es ein $g \in W(L)$ mit $(\alpha g, \beta) \neq 0$. Ersetzt man αg durch α so kann man o.B.d.A. annehmen, dass $(\alpha, \beta) \neq 0$ gilt. Ersetzt man weiter α durch $-\alpha = \alpha\sigma_\alpha$, so kann man außerdem annehmen, dass $(\alpha, \beta) > 0$. Dann ist aber entweder $\alpha = \beta$ oder $(\alpha, \beta) = 1$ und $v := \alpha - \beta \in R(L)$. Im zweiten Fall ist

$$\alpha\sigma_v = \alpha - (v, \alpha)v = \alpha - (\alpha - \beta) = \beta.$$

Also operiert $W(L)$ wie gewünscht transitiv auf $R(L)$. $\square$

Der Zusammenhang der beiden Kapitel über Wurzelgitter und die Weyl-Gruppe werden in folgender Äquivalenzaussage deutlich:

(3.4) Satz
Sei $L \subset \mathbb{R}^n$ ein irreduzibles Wurzelgitter. Dann sind die folgenden Aussagen äquivalent:

(i) L enthält n paarweise orthogonale Wurzeln.

(ii) $n\mathbb{A}_1 = \mathbb{A}_1 \oplus \ldots \oplus \mathbb{A}_1 \subset L$.

(iii) $-\operatorname{id} \in W(L)$.

(iv) $2L^\# \subset L$.

(v) L ist bis auf Isometrie $\mathbb{A}_1, \mathbb{D}_n$ ($n \geq 4$, n gerade), $\mathbb{E}_7$, $\mathbb{E}_8$.

Beweis
Da der Beweis von (v) nach (iv) mittels einer anderen äquivalenten Aussage aus der Codierungstheorie geführt wird, wird dieser hier weggelassen, da eine Ausführung über die Grundlagen von Codes den Rahmen sprengen würde. (vgl. Ebeling Prop. 1.5.) $\square$

Literatur

[1] Wolfgang Ebeling: Lattices and Codes
Vieweg Wiesbaden Braunschweig, 2002

[2] Gabriele Nebe: Skript zur Vorlesung Gitter und Codes
online erschienen, 2008/2009